(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 November 2002 (07.11.2002)

PCT

(10) International Publication Number
WO 02/089444 A1

(51) International Patent Classification[7]: H04L 29/06, 9/32, G07F 7/10

(21) International Application Number: PCT/EP02/03929

(22) International Filing Date: 9 April 2002 (09.04.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/844,246 30 April 2001 (30.04.2001) US
09/844,439 30 April 2001 (30.04.2001) US

(71) Applicant *(for all designated States except US)*: **ACTIV-CARD** [FR/FR]; 24-28, avenue du Général de Gaulle, F-92156 Suresnes Cedex (FR).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **AUDEBERT, Yves, Louis, Gabriel** [FR/US]; 237 Forrester Road, Los Gatos, CA 95032 (US). **CLEMOT, Olivier** [FR/FR]; 23, rue Jules Parent, F-92500 Rueil-Malmaison (FR).

(74) Agent: **CABINET JP COLAS**; 37, avenue Franklin D. Roosevelt, F-75008 Paris (FR).

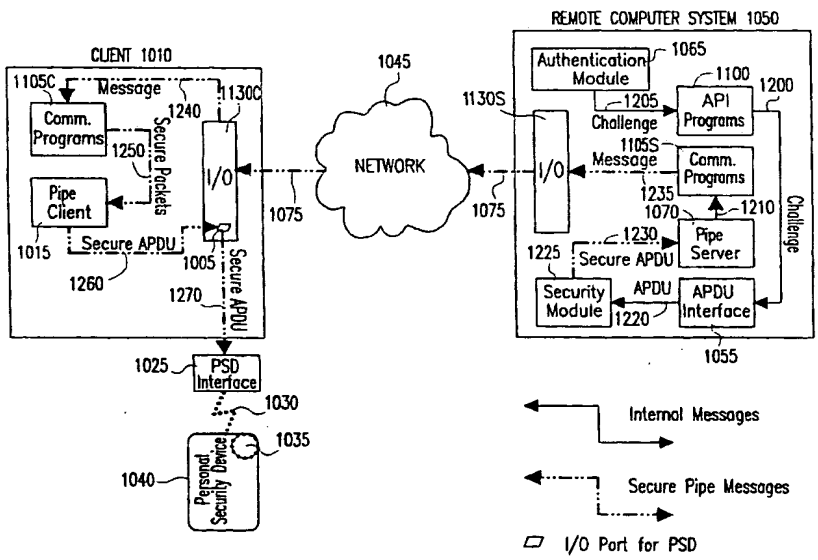
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR AUTHENTICATING A PERSONAL SECURITY DEVICE VIS-A-VIS AT LEAST ONE REMOTE COMPUTER SYSTEM



(57) Abstract: The present invention provides a method for authenticating at least one Personal Security Device PSD (1040) vis-ô-vis at least a first Remote Computer System (1050) over a first network (1045) using at least one Client (1010) as a host to said at least one PSD (1040), said method comprising the steps of: a) establishing at least one communications pipe (1075) over said first network (1045) between said at least one PSD (1040) and said at least first Remote Computer System (1050); and b) running a challenge/response process between said Remote Computer System (1050) and said at least one PSD (1040) through said at least one communications pipe (1075).

WO 02/089444 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHOD AND SYSTEM FOR AUTHENTICATING A PERSONAL SECURITY DEVICE VIS-À-VIS AT LEAST ONE REMOTE COMPUTER SYSTEM

1. Field of Invention

The present invention relates to a method and system for authenticating a Personal Security Device (PSD) vis-à-vis at least one Remote Computer System. More particularly, the present invention relates to a method and system for authenticating a Personal Security Device (PSD) vis-à-vis a plurality of Remote Computer Systems.

2. Background of Invention

One of the simplest and most commonly used authentication methods employed is the static password, whereby a Client computer challenges an end user for a pre-determined password. Once the end user provides the correct password, access is permitted to secure functions or data available on one or more Remote Computer Systems. A significant limitation of the current art is that localized authentication transactions are potentially vulnerable to compromise by unauthorized programs running on the local Client or by other illicit means intending to monitor the password authentication process. In a single point authentication process, once a point of entry to a network is compromised, all locations using the same security codes are generally compromised as well.

One security method commonly used to overcome single point authentication failures employs the use of separate static passwords for each pre-determined secure resource. While this method is an improvement over a single multi-use password, this method is still vulnerable to illicit password monitoring, requires an end user to remember multiple passwords, and inefficiently ties up network resources by repeating the entire authentication process each time access to a different secure resource is requested.

Also, as a practical consideration, requiring an end user to remember several different passwords typically results in the same password being used for all secure resources, hence defeating the entire purpose of performing multiple authentications using static passwords.

A more sophisticated approach than the previously described methods, involves the use of Personal Security Devices (PSD) such as smart cards, which allows storage of multiple credentials, passwords, certificates, private keys, etc. By implementing the use of smart cards, the ability to compromise passwords is significantly reduced. However, PSDs are still somewhat vulnerable to illicit monitoring during transactions with local

Client. An additional limitation of this method becomes apparent when attempting to perform multiple authenticating transactions using a single PSD over a network connection. The PSD, beings a slow serial device, only allows one transaction to occur at a time. In addition, network contention and processor execution speed issues become particularly problematic when low bandwidth connections (e.g. dialup connections) are made between a Client and a Remote Computer System during authentication with the PSD.

3. Summary of Invention

It is an object of the present invention to provide a more secure method for authenticating a PSD vis-à-vis at least one Remote Computer System.

This object is achieved with a method for authenticating at least one PSD vis-à-vis at least a first Remote Computer System over a first network using at least one Client as a host to said at least one PSD, said method comprising the steps of :

- a) establishing at least one communications pipe over said first network between said at least one PSD and said at least first Remote Computer System (1050),
- b) generating or retrieving, in said at least first Remote Computer System, a first authentication challenge as a PSD-formatted message,
- c) transmitting said first authentication challenge from said at least first Remote Computer System (1050) to said at least one PSD through said at least one communications pipe,
- d) challenging said at least one PSD with said first authentication challenge, thereby generating a first authentication response as a PSD-formatted message,
- e) transmitting said first authentication response from said at least one PSD to said at least first Remote Computer System through said at least one communications pipe, and
- f) authenticating, in said at least first Remote Computer System, said first authentication response.

With this method, sensitive data processing is performed only within the Remote Computer System(s), i.e. in highly secure and protected domain(s), which greatly reduces the chances of unauthorized access or interception.

It is another object of the present invention to facilitate multiple authenticating transactions between a single PSD and a plurality or Remote Computer Systems.

According to a first embodiment, this other object of the invention can be achieved with a method according for authenticating said at least one PSD vis-à-vis at least one subsequent Remote Computer System which is functionally connected to said at least first Remote Computer System through a second network, said method comprising, in addition to the above-mentioned steps, the further steps of :

- aa) generating or retrieving, in said at least one subsequent Remote Computer System, a second authentication challenge,
- ab) transmitting said second authentication challenge from said at least one subsequent Remote Computer System to said at least first Remote Computer System via said second network,
- ac) converting said second authentication challenge in a PSD-formatted message,
- ad) transmitting said second authentication challenge from said at least first Remote Computer System to said at least one PSD through said at least one communications pipe,
- ae) challenging said at least one PSD with said second authentication challenge, thereby generating a second authentication response,
- af) transmitting said second authentication response from said at least one PSD to said at least first Remote Computer System through said at least one communications pipe,
- ag) transmitting said second authentication response from said at least first Remote Computer System to said at least one subsequent Remote Computer System via said second network, and
- ah) authenticating, in said at least one subsequent Remote Computer System, said second authentication response.

According to a second embodiment, said other object of the invention can be achieved with a method for authenticating said at least one PSD vis-à-vis at least one subsequent Remote Computer System which is functionally connected to said at least first Remote Computer System through a second network, said method comprising, in addition to the above-mentioned steps, the further steps of :

- ba) sending to said at least one PSD a credentials transfer command,
- bb) transmitting credentials from said at least one PSD to said at least first Remote Computer System through said at least one communications pipe,
- bc) storing said credentials in said at least first Remote Computer System,

- bd) generating or retrieving, in said at least one subsequent Remote Computer System, a second authentication challenge,

- be) transmitting said second authentication challenge from said at least one subsequent Remote Computer System to said at least first Remote Computer System via said second network,

- bf) challenging said stored credentials with said second authentication challenge, thereby generating a second authentication response,

- bg) transmitting said second authentication response from said at least first Remote Computer System to said at least one subsequent Remote Computer System via said second network, and

- bh) authenticating, in said at least one subsequent Remote Computer System, said second authentication response.

In said first and second embodiments, the first Remote Computer System establishing and maintaining the communications pipe with the PSD performs an initial authentication, and then acts as a secure hub and Client authentication proxy for subsequent Remote Computer Systems requesting Client authentication.

In a multi-tasking operating environment, multiple authentications occur as background transactions, which are transparent to the end user. The Remote Computer System acting as a secure hub may form multiple communications pipes with other Clients connected to a network. Authentication transactions will occur more rapidly and seamlessly, since Remote Computer Systems are generally provided with greater network bandwidth and processing power than local Clients.

By relocating the authentication process to a Remote Computer System acting as a secure hub, a more simplified means to perform end-to-end authentication and maintain an audit trail of transactions by authenticated end users and transactions with subsequent Remote Computer Systems is readily accomplished since all authentication transactions are routed through the Remote Computer System acting as a secure hub.

In said first embodiment of the invention, the Remote Computer System acting as a secure hub performs the initial Client authentication and then routes subsequent authentication challenges through the communications pipe to the PSD for processing within the PSD, then returns the PSD generated authentication response back through the communications pipe over a network and to the challenging Remote Computer System.

In said second embodiment of the invention, the Remote Computer System acting as a secure hub performs the initial Client authentication and then copies, if not already present, the PSD's authentication credentials through the communications pipe to a

secure storage location within the secure hub. The secure hub using the transferred PSD credentials and equivalent algorithms authenticates the Client to subsequent Remote Computer Systems by emulating the PSD.

In both of said embodiments, communications between local Clients and Remote Computers Systems over one or more networks can employ secure communications protocols, such as TCP/IP with Secure Socket Layer (SSL) encryption, IPSEC, etc., which further reduces the likelihood of unauthorized access or interception. For non-proprietary transactions with the PSD, secure communications are optional.

Additional security improvements may be facilitated by establishing a secure communications pipe between the PSD and the Remote Computer System acting as a secure hub, i.e. a communications pipe in which end-to-end cryptographic means are involved (see section 5.1.2. below).

Such cryptographic means can be implemented by software-based security mechanisms or by a Hardware Security Module (HSM) functionally connected to the Remote Computer System acting as a secure hub.

It is another object of the invention to provide a system for implementing the above-mentioned method.

4. Brief Description of Drawings

FIG. 1 is a generalized system block diagram for implementing a plain communications pipe,

FIG. 2 is a detailed block diagram depicting initiating a plain communications pipe,

FIG. 3 is a detailed block diagram depicting establishing a plain communications pipe,

FIG. 4A is a generalized system block diagram for implementing a secure communications pipe which includes software-based security mechanisms,

FIG. 4B is a generalized system block diagram for implementing a secure communications pipe which includes HSM-based security mechanisms,

FIG. 5 is a detailed block diagram depicting initiating a secure communications pipe,

FIG. 6 is a detailed block diagram depicting establishing a secure communications pipe,

FIG. 7 is a general system block diagram for implementing the authentication of a PSD vis-à-vis at least one Remote Computer System,

FIG. 8 is a detailed block diagram illustrating initial authentication challenge (first embodiment of the invention),

FIG. 9 is a detailed block diagram illustrating initial authentication response (first embodiment of the invention),

FIG. 10 is a detailed block diagram illustrating remote authentication challenge (first embodiment of the invention),

FIG. 11 is a detailed block diagram illustrating remote authentication response (first embodiment of the invention),

FIG. 12 is a detailed block diagram illustrating authentication credential transfer (second embodiment of the invention),

FIG. 13 is a detailed block diagram illustrating remote authentication challenge (second embodiment of the invention),

FIG. 14 is a detailed block diagram illustrating remote authentication (second embodiment of the invention).

5. Detailed Description of the Invention

In a first part (section 5.1.), the present Detailed Description of the Invention will disclose how to establish a plain communications pipe and a secure communications pipe between a PSD and a Remote Computer System, generally speaking.

In a second part (section 5.2.), the present Detailed Description of the Invention will disclose how to enhance security of an authentication process of a PSD vis-à-vis a Remote Computer System using said secure communications pipe, and how to use said Remote Computer System as a secure hub for authentication of said PSD vis-à-vis a plurality of subsequent Remote Computer Systems.

Said second part of the Detailed Description will be based on the use of a secure communications pipe, but the present invention is not limited to such a use.

The use of a plain communications pipe, i.e. of a communications pipe which does not involve end-to-end cryptographic mechanisms, falls within the scope of the present invention.

Note also that the following description of the invention will be based on a PSD which receives and sends APDU-(Application Protocol Data Unit)-formatted messages.

APDU messaging format, which is *per se* known in the art, is a lower-level messaging format which allows a PSD to communicate with higher-level applications located in devices to which the PSD is to be connected.

It must be clear that the present invention is not limited to the use of an APDU messaging format, and that any other low-level messaging format that can be processed by the PSD enters within the scope of the present invention.

In the appended claims, a message having such a format will be designated by the generic expression "PSD-formatted message".

5.1. Establishment of a Communications Pipe

5.1.1. Plain Communications Pipe

Referring to FIG. 1, a generalized system block diagram of the architectures of a Client 10 and of a Remote Computer System 50 is shown. The various layers shown are based on the Open System Interconnection model (OSI). For simplicity, certain layers common to both the Client and Remote Computer System are not shown and should be assumed to be present and incorporated into adjacent layers. The layers common to both a Client and Remote Computer System include:

- an Applications Layer 90 which generally contains higher level software applications (e.g. word processor) and a user interface and such as a Graphical User Interface (GUI),

- an Applications Programming Interface (API) Layer 100 for processing and manipulating data for use by either higher or lower level applications,

- a Communications Layer 105 which contains communications programs including secure communications capabilities, which enable a Client to communicate with a Remote Computer System to exchange information in an agreed upon protocol and visa versa,

- an Operating System Layer 110 or equivalent runtime environment, which controls the allocation and usage of hardware resources such as memory, Central Processing Unit (CPU) time, disk space, hardware I/O port assignments, peripheral device management,

- a Hardware Drivers Layer 120 which permits the operating system to communicate and control physical devices connected to the Client's or Remote Computer System's hardware I/O bus,

- and a Physical Device Layer 130 where Network Interface Cards (NIC) 140 provide the physical connections to a telecommunications network 45. Other Hardware Devices 80 may also be connected at this Layer.

5.1.1.1. Client Specific Features

A specialized program contained within the API Layer 100 of the Client and referred to as a Pipe Client 15, interacts with Communications Programs contained within the Communications Layer 105. The Pipe Client 15 functions to separate encapsulated APDU requests from incoming messaging packets received from a network 45 for processing by a locally connected PSD 40. Alternately, outbound APDU responses generated by a locally connected PSD 40, are processed by the Pipe Client for encapsulation into an agreed upon communications protocol by Communications Programs contained within the Communications Layer 105.

A software driver contained within the Communications Layer 105 of the Client and referred to as a PSD Software Interface 20 directs incoming APDUs communicated by the Pipe Client 15 into the I/O device port connecting the PSD Hardware Device Interface 25 to the locally connected PSD 40. Outgoing APDUs generated by the PSD are communicated through the PSD Hardware Device Interface 25 through the I/O device port to the PSD Software Interface 20 and subsequently communicated to the Pipe Client 15.

5.1.1.2. Remote Computer System Specific Features

A first specialized program contained within the API Layer 100 of the Remote Computer System 50 and referred to as an APDU Interface 55, translates higher level messaging formats into low-level APDU messaging format required to communicate with a PSD 40. Alternately, the APDU Interface 55 translates incoming APDU responses received from a PSD 40 into higher level messaging formats used by programs in the API Layer 100 and Applications Layer 90 of the Remote Computer System.

A second specialized program contained within the API Layer 100 of the Remote Computer System 50 and referred to as a Pipe Server 70 interacts with Communications Programs contained within the Communications Layer 105. The Pipe Server 70 functions

to separate encapsulated APDU requests from incoming messaging packets received from a network 45 for processing by the APDU Interface 55. Alternately, outbound APDU requests translated by the APDU Interface 55 are processed by the Pipe Server for encapsulation into an agreed upon communications protocol by Communications Programs contained within the Communications Layer 105.

5.1.1.3. Other Features

The connection 30 between the PSD 40 and PSD Hardware Interface 25 includes but is not limited to traditional electrical or optical fiber connections or wireless means including optical, radio, acoustical, magnetic, or electromechanical. Likewise the connection 75 between the Client 10 and the network 45, and the connection 75 between the Remote Computer System 50 and the network 45 may be accomplished analogously.

The network, shown generally at 45, includes both public and private telecommunications networks connected by traditional electrical, optical, electro-acoustical (DTMF) or by other wireless means. Any mutually agreed upon communications protocol capable of encapsulating APDU commands may be employed to establish a plain communications pipe including open or secure communications protocols.

Referring now to FIG. 2, depicts initiating a plain communications pipe between the Remote Computer System 50 and the PSD 40 connected to a Client 10. In this depiction, the Remote Computer System 50 is sending a request to PSD 40 for non-proprietary embedded information 35, for example an identification number. PSD 40 is connected 30 to the local Client 10 using PSD Interface 25. PSD Interface 25 communicates with the Client 10 via hardware device port 5.

To initiate a plain communications pipe between Remote Computer System 50 and PSD 40, the Remote Computer System 50 generates a request 200 by way of API programs 100 which is translated into APDU format 220 by the APDU Interface 55 and sent to the Pipe Server 70 for message encapsulation. The encapsulated APDUs are then sent 210 to the Communications Programs 105S for incorporation into outgoing message packets 230.

The message packets 230 containing the encapsulated APDUs are transmitted 75 over the network 45 via a Network Interface Card (I/O) 130S. The Client 10 receives the message packets 240 containing the encapsulated APDUs which are received from the network 45 via a Network Interface Card (I/O) 130C installed on the local Client. The incoming messages are processed by Client-side Communications Programs 105C and

routed 250 into the Pipe Client 15 for APDU extraction. The extracted APDUs are sent 260 through hardware device port 5, routed 270 into the PSD Interface 25 and sent to PSD 40 via connection 30 for processing within PSD domain 35.

Alternative requests to form a plain communications pipe 75 between a Remote Computer System 50 and a PSD 40 may be initiated by Client 10 requesting access to information contained on one or more networked local Clients, by connecting a PSD 40 to PSD Interface 25 which initiates a request to form a plain communications pipe 75, or by another Remote Computer System requesting access to PSD 40.

Referring now to FIG. 3, depicts a PSD response which establishes the plain communications pipe between PSD 40 and Remote Computer System 50. In this depiction, the request previously received is processed within the PSD domain 35, which generates a response message. The PSD response is sent in APDU format from PSD 40 through connection 30 and into PSD interface 25. The PSD response is then routed 370 through hardware device port 5 and sent 360 to the Pipe Client 15 for processing and encapsulation. The resulting message packets are then sent 350 to the Client-side Communications Programs 105C for incorporation into outgoing message packets 340. The message packets 340 containing the encapsulated APDUs are transmitted 75 over the network 45 via the Network Interface Card (I/O) 130C.

The Remote Computer System 50 receives the message packets 330 containing the encapsulated APDUs, which are received from the network 45 via the Network Interface Card (I/O) 130S installed on the Remote Computer System. The incoming messages are processed by server-side Communications Programs 105S and routed 310 into the Pipe Server 70 for APDU extraction. The extracted APDUs are sent 320 to the APDU Interface 55 for processing and translation into a higher-level format and sent 300 to API Level programs 100 for processing and further transactions with the PSD 40 if desired.

5.1.2. Secure communications pipe

Referring now to FIG. 4A, a generalized system block diagram of one implementation of a secure communications pipe is shown. The general system block diagram includes an additional software-based Cryptography Module 470 installed on the Remote Computer System, which is not shown in FIG. 1.

FIG. 4B depicts an alternative to using software-based security mechanisms. In this alternative, a Hardware Security Module (HSM) 440 is employed to perform cryptographic functions. To access the HSM, a software driver referred to as an HSM

S/W Interface 475, is included in the API Layer 100. The HSM software driver communicates with a physical device interface included in the Physical Device Layer 130. The physical device interface is installed on the I/O bus of the Remote Computer System, and is referred to as an HSM H/W Interface 485. The HSM module 440 is connected 430 to the HSM H/W Interface in a manner analogous to the PSD connection to the PSD Interface previously described. The use of HSM technologies provides end-to-end security, which further reduces the possibility of unauthorized disclosure of cryptographic or sensitive information.

Both APDU messaging security mechanisms shown in FIGs. 4A & 4B are used to generate cryptographic keys necessary to unlock secure functions and data contained within the secure domain of a PSD, encrypt outgoing APDUs and decrypt incoming encrypted APDUs. The security mechanisms employed in generating a secure pipe may include synchronous, asynchronous or any combination of cryptography methods.

Secure communications protocols used to communicate over a network are accomplished by the Communications Programs contained within the Communications Layers 105. Cryptography used in generating secure communications may employ the security mechanisms described for APDU messaging, employ separate mechanisms or employ any combination thereof.

Referring now to FIG. 5, depicts the initiating of a secure pipe between the Remote Computer System and the PSD 40 connected to Client 10. In this depiction, Remote Computer System 50 is sending a secure request to PSD 40 for proprietary embedded information 35, for example an authentication password. PSD 40 is connected 30 to the local Client 10 using PSD Interface 25. PSD Interface 25 communicates with the Client 10 via hardware device port 5.

To initiate a secure communications pipe between Remote Computer System 50 and PSD 40, a request 500 is generated on Remote Computer System 50 to access PSD 40 by way of API programs 100 which are translated into APDU format by the APDU Interface 55. The APDUs are then sent 520 to a Security Module 525 for encryption using a pre-established cryptography method. The proper cryptographic parameters may be determined by using a look-up table or database, which cross-references the PSD's unique internal identification information with one or more codes necessary to implement the appointed cryptography method.

The encrypted APDUs are then routed 510 to the Pipe Server 70 for message encapsulation. The encapsulated APDUs are then sent 530 to the Communications Programs 105 for processing, encryption using a pre-established secure communications protocol and incorporation into outgoing message packets 535. The secure message

packets 535 containing the encrypted and encapsulated APDUs are transmitted 75 over the network 45 via a Network Interface Card (I/O) 130S.

The Client 10 receives the message packets 540 containing the encrypted and encapsulated APDUs which are received from the network 45 via a Network Interface Card (I/O) 130C installed on the local Client 10.

The incoming encrypted message packets are decrypted and processed using the pre-established cryptography employed in the secure communications protocol by Client-side Communications Programs 105C. The unencrypted message packets still containing the encrypted APDUs are routed 550 into the Pipe Client 15 for APDU extraction. The extracted APDUs are sent 560 through hardware device port 5, routed 570 into the PSD Interface 25 and sent to PSD 40 via connection 30 for decryption and processing within the secure domain 35 of the PSD 40. Using a pre-established cryptography method, incoming secure APDUs are decrypted and requests processed.

Referring now to FIG. 6, depicts a PSD secure response, which establishes the secure communications pipe between PSD 40 and Remote Computer System 50. In this depiction, the secure request previously received is processed within the secure domain 35 of the PSD 40, which causes the PSD to generate a secure response message using a pre-established cryptography method.

The PSD secure response is sent in APDU format from PSD 40 through connection 30 and into PSD interface 25. The PSD secure response is then routed 670 through hardware device port 5 and sent 660 to the Pipe Client 15 for processing and encapsulation. The resulting message packets are then sent 650 to the Client-side Communications Programs 105 for processing, encryption using a pre-established secure communications protocol and incorporation into outgoing message packets 640. The message packets 640 containing the encapsulated APDUs are transmitted 75 over the network 45 via the Network Interface Card (I/O) 130C.

The Remote Computer System 50 receives the message packets 635 containing the encapsulated APDUs from the network 45 via the Network Interface Card (I/O) 130S installed on the Remote Computer System 50. The incoming messages are processed and decrypted using the pre-established cryptography method employed in the secure communications protocol by the server-side Communications Programs 105 and routed 610 into the Pipe Server 70 for secure APDU extraction. The extracted secure APDUs are sent 630 to the Security Module 525 for decryption of the secure APDUs using the pre-established cryptography method. The decrypted APDUs are then routed 620 to the APDU Interface 55 for processing and translation into a higher-level format and sent 600 to API programs 100 for processing and further transactions with the PSD 40 if desired.

This step establishes the secure "pipe" to communicate with the PSD. The secure pipe is maintained until the Remote Computer System signals the Client to close the hardware interface port 5.

No limitation is intended in the number of PSDs and Clients forming communications pipes 75 with one or more Remote Computer System(s) 50, nor should any limitation on the number of Remote Computer Systems 50 available for generating communications pipes 75 be construed from the drawings. Lastly, no limitation is intended concerning the initiating event to establish a communications pipe.

5.2. Authentication method and system using a communications pipe

As already mentioned above, description of said authentication method and system will be based on the use of a secure communications pipe, but the present invention is not limited to such a use.

The use of a plain communications pipe falls within the scope of the present invention.

The steps involved in performing authentication through a secure communications pipe are shown in Figures 7 through 14. Figure 7 is a generalized system block diagram. Figures 8 through 11 illustrate a first embodiment of the invention where responses to authentication challenges are generated within the secure domain of a Personal Security Device. Figures 12 through 14 illustrate a second embodiment of the invention where a Remote Computer System acting as a secure hub provides the proper response to authentication challenges, rather than directing challenges through the communications pipe into the PSD for processing. Characters shown with a prime sign (e.g. C') indicate a duplicate of an original authentication credential. Other drawing details shown but not described refer to information described in previous section 5.1.

Referring now to FIG. 7, a generalized system block diagram of the invention is depicted, where a Personal Security Device 1040 is connected to a Client 1010 which is itself connected over a network 1045 to a Remote Computer System 1050 using a secure communications pipe 1075 as described in previous section 5.1.2. Remote Computer System 1050 is operating as a secure hub following initial authentication as described below, to service authentication requests made by subsequent Remote Computer Systems sent over a network 1045 or 1045A.

The subsequent Remote Computer System 1150 is an example of a system requiring authentication when a request for secure functions or data is sent from Client computer 1010 over the networks 1045 and 1045A. The secure communications pipe

1075 applies to authentication transactions but does not restrict nor control non-secure transactions occurring over either network 1045 or 1045A.

Networks 1045 and 1045A may be a common network as in a virtual private networking arrangement or separate networks such as private intranet and public internet arrangements. The networks 1045 and 1045A are depicted separately for illustrative purposes only. No limitation is intended in the number of PSDs and Clients forming communications pipes 1075 with one or more secure hubs 1050; nor should any limitation on the number of subsequent Remote Computer Systems 1150 available for authentication be construed from the drawing. Transactions not involving authentications are not restricted to the secure hub.

The basic operation of the secure hub may be initiated when an end user at a Client requests access to secure functions or data contained on one or more Remote Computer Systems connected by a network. An available Remote Computer System, in which a secure communications pipe has been established as described in previous section 5.1.2., authenticates the end user and Client using the security mechanisms contained within the secure domain of the PSD. Alternatively, an external event such as a need to update information within a PSD may trigger a subsequent Remote Computer System to initiate the authentication process.

Once an initial Client authentication has been accomplished by the available Remote Computer System, subsequent authentication challenges transmitted over a network 1045 or 1045A made by subsequent Remote Computer Systems are directed to the Remote Computer System 1050 acting as a secure hub and depending on which embodiment of the invention employed, are either routed through the appropriate communications pipe 1075 to PSD 1040 or are directly authenticated by the Remote Computer System 1050.

5.2.1. First embodiment of the invention

Referring to FIG. 8, to establish a secure hub, a Client 1010 causes an authentication challenge to be generated on a Remote Computer System 1050, by requesting access to secure functions or data over a network 1045. Upon receiving the request from Client 1010, the Remote Computer System 1050 generates an authentication challenge 1205 within a secure domain designated as authentication routine 1065. The authentication challenge is processed by an API level program 1100 and routed 1200 to an APDU interface 1055 for translation into an APDU format. The APDUs are then sent 1220 to a Security Module 1225 for encryption. The encrypted

APDUs are then routed 1230 to a Pipe Server 1070 for encapsulation into outgoing messaging and sent 1210 to the Communications Programs 1105S for transmission over the communications pipe 1075, through the network 1045 into the network interface 1130C of the Client 10. The incoming messages are then routed 1240 to Communications Programs 1105C for processing.

Following processing, the messages are sent 1250 to a Pipe Client 1015 for separation of the encapsulated APDUs. The APDUs are then sent 1260 through a hardware device port 1005 assigned to a PSD Interface 1025. PSD Interface 1025 routes the incoming APDUs into the PSD 1040 via connection 1030, where it is subsequently decrypted and processed within its secure domain 1035.

Referring to FIG. 9, once PSD 1040 has processed the authentication challenge within the secure domain 1035 of the PSD, an authentication response message is generated using a pre-established cryptography method.

The authentication response is sent in APDU format from PSD 1040 through connection 1030 and into PSD interface 1025. The PSD secure response is then routed 1370 through hardware device port 1005 and sent 1360 to the Pipe Client 1015 for processing and encapsulation. The resulting message packets are then sent 1350 to the Client-side Communications Programs 1105C for processing, encryption using a pre-established secure communications protocol and incorporation into outgoing message packets 1340. The message packets 1340 containing the encapsulated APDUs are transmitted 1075 over the network 1045 via a network interface card (I/O) 1130C.

The Remote Computer System 1050 receives the message packets 1335 containing the encapsulated APDUs from the network 1045 via a network interface card (I/O) 1130S installed on the Remote Computer System. The incoming messages are processed and decrypted using the pre-established cryptography method employed in the secure communications protocol by the server-side Communications Programs 1105S and routed 1310 into the Pipe Server 1070 for secure APDU extraction. The extracted secure APDUs are sent 1330 to the Security Module 1325 for decryption of the secure APDUs using the pre-established cryptography method. The decrypted APDUs are then routed to the APDU Interface 1055 for processing and translation into a higher-level format and sent 1300 to API Level programs 1100 for processing. If authentication is successful, the Remote Computer System 1050 allows access to secure functions or data and establishes itself as a secure hub. If authentication fails, the end user will be unable to access secure functions or data.

Referring to FIG. 10, once the secure hub has been established as previously described, remote authentication of subsequent Remote Computer Systems may be

accomplished. Remote authentication may be initiated either by a Client's request for access to secure functions or data or by other Remote Computer Systems to perform transactions within the secure domain of a PSD.

To perform a remote authentication, a challenge 1085 is issued by a subsequent Remote Computer System 1150. The challenge is routed over a network 1045, into the secure hub 1050. The incoming challenge is processed and decrypted in the secure hub 1050 using the pre-established cryptography method employed in the secure communications protocol by the server-side Communications Programs 1105S and routed 1085 to an API level program 1100 where it is processed and routed 1400 to an APDU interface 1055 for translation into an APDU format. The APDUs are then sent 1420 to a Security Module 1425 for encryption. The encrypted APDUs are then routed 1430 to a Pipe Server 1070 for encapsulation into outgoing messaging and sent 1410 to the communications programs 1105S for transmission over the communications pipe 1075, through the network 1045 into the network interface 1130C of the Client 1010.

The incoming messages are then routed 1440 to Communications Programs 1105C for processing. Following processing, the messages are sent 1450 to a Pipe Client 1015 for separation of the encapsulated APDUs. The APDUs are then sent 1460 through a hardware device port 1005 assigned to a PSD Interface 1025. PSD Interface 1025 routes the incoming APDUs into the PSD 1040 via connection 1030, where it is subsequently decrypted and processed within its secure domain 1035.

Referring to FIG. 11, once PSD 1040 has processed the authentication challenge within its secure domain 1035, an authentication response message is generated using a pre-established cryptography method. The authentication response is sent in APDU format from PSD 1040 through connection 1030 and into PSD interface 1025. The PSD secure response is then routed 1570 through hardware device port 1005 and sent 1560 to the Pipe Client 1015 for processing and encapsulation. The resulting message packets are then sent 1550 to the Client-side Communications Programs 1105C for processing, encryption using a pre-established secure communications protocol and incorporation into outgoing message packets 1540. The message packets 1540 containing the encapsulated APDUs are transmitted 1075 over the network 1045 via network interface card (I/O) 1130C.

The secure hub 1050 receives the message packets 1535 containing the encapsulated APDUs from the network 1045 via network interface card (I/O) 1130S. The incoming messages are processed and decrypted using the pre-established cryptography method employed in the secure communications protocol by the server-side Communications Programs 1105S and routed 1510 into the Pipe Server 1070 for secure

APDU extraction. The extracted secure APDUs are sent 1530 to the Security Module 1525 for decryption of the secure APDUs using the pre-established cryptography method. The decrypted APDUs are then routed 1520 to the APDU Interface 1055 for processing and translation into a higher-level format and sent 1500 to API Level programs 1100 for processing. Authentication Module 1065 within the secure hub 1050 remains inactive during the transfer of authentication information. The authentication response message is then routed 1085 into the Communications Programs 1105S where the response is sent over the network 1045 in a pre-established secure communications protocol to the challenging subsequent Remote Computer System 1150.

The incoming response message is decrypted and sent to an Authentication Module 1095. If authentication is successful, the subsequent Remote Computer System 1150 allows access to secure functions or data. If authentication fails, the end user will be unable to access secure functions or data.

5.2.2. Second embodiment of the invention

Referring to FIG. 12 depicts an alternate embodiment of the current invention where the Remote Computer System 1050 transfers copies of the PSD credentials C 1035, if not pre-existing on said Remote computer System 1050. To perform credential transfer, an initial authentication transaction is performed by the Remote Computer System 1050 as previously described. Following authentication, additional commands are sent by the Remote Computer System 1050 to transfer the specified credentials.

The credentials are generated using a pre-established cryptography method and sent in APDU format from PSD 1040 through connection 1030 and into PSD interface 1025. The PSD secure response is then routed 1670 through hardware device port 1005 and sent 1660 to the Pipe Client 1015 for processing and encapsulation. The resulting message packets are then sent 1650 to the Client-side Communications Programs 1105C for processing, encryption using a pre-established secure communications protocol and incorporation into outgoing message packets 1640. The message packets 640 containing the encapsulated APDUs are transmitted 1075 over the network 1045 via a network interface card (I/O) 1130C.

The Remote Computer System 1050 receives the message packets 1635 containing the encapsulated APDUs from the network 1045 via network interface card (I/O) 1130S installed on the Remote Computer System.

The incoming messages are processed and decrypted using the pre-established cryptography method employed in the secure communications protocol by the server-side

Communications Programs 1105S and routed 1610 into the Pipe Server 1070 for secure APDU extraction. The extracted secure APDUs are sent 1630 to the Security Module 1625 for decryption of the secure APDUs using the pre-established cryptography method. The decrypted APDUs are then routed 1620 to the APDU Interface 1055 for processing and translation into a higher-level format and sent 1600 to API Level programs 1100 for processing and subsequently sent 1605 to the Authentication Module 1065 for secure storage and future use. The transferred authentication information is shown in FIG. 12 as C'.

In FIG. 13, an authentication challenge 1085 is sent by a subsequent Remote Computer System 1150 over a network 1045. The Remote Computer System 1050 acting as a secure hub receives the incoming challenge 1085 from the network 1045 via network interface card 1130S installed on the Remote Computer System 1050. The incoming challenges 1085 are processed and decrypted using the pre-established cryptography method employed in the secure communications protocol by the server-side Communications Programs 1105S and routed to API Level programs 1100 for processing. The processed challenge is then sent 1705 to the Authentication Module 1065 for authentication using the PSD's transferred credentials C' 1035'. The communications pipe 1075 may remain intact during this process to allow for other transactions to occur.

Referring to FIG. 14, the secure hub 1050 generates an authentication reply within the Authentication Module 1065 which is sent 1805 to the API Level Programs 1100 for processing, and subsequently routed 1810 to the Server-side Communications Programs 1105S for processing, encryption using a pre-established secure communications protocol and incorporation into outgoing message packets. The message packets are routed over the network 1045 to the challenging subsequent Remote Computer System 1150. The incoming messages are then decrypted and the authentication reply processed by an internal authentication module 1095. If authentication is successful, the subsequent Remote Computer System 1150 allows access to secure functions or data. If authentication fails, the end user will be unable to access secure functions or data.

The foregoing described embodiments of the invention are provided as illustrations and descriptions. They are not intended to limit the invention to precise form described. In particular, it is contemplated that functional implementation of the invention described herein may be implemented equivalently in hardware, software, firmware, and/or other available functional components or building blocks. Other variations and embodiments are possible in light of above teachings, and it is not intended that the scope of the invention be limited by this Detailed Description, but rather by the Claims following herein.

CLAIMS

What is claimed is :

1. A method for authenticating at least one PSD (1040) vis-à-vis at least a first Remote Computer System (1050) over a first network (1045) using at least one Client (1010) as a host to said at least one PSD (1040), said method comprising the steps of :

- a) establishing at least one communications pipe (1075) over said first network (1045) between said at least one PSD (1040) and said at least first Remote Computer System (1050),

- b) generating or retrieving, in said at least first Remote Computer System (1050), a first authentication challenge (1205) as a PSD-formatted message (1220),

- c) transmitting said first authentication challenge (1205) from said at least first Remote Computer System (1050) to said at least one PSD (1040) through said at least one communications pipe (1075),

- d) challenging said at least one PSD (1040) with said first authentication challenge, thereby generating a first authentication response as a PSD-formatted message (1370),

- e) transmitting said first authentication response from said at least one PSD (1040) to said at least first Remote Computer System (1050) through said at least one communications pipe (1075), and

- f) authenticating, in said at least first Remote Computer System (1050), said first authentication response (1305).

2. The method according to claim 1, further comprising the steps of:

- b1) encrypting said first authentication challenge (1205) in said at least first Remote Computer System (1050) after said step b) and before said step c),

- c1) decrypting said first authentication challenge in said at least one PSD (1040) after said step c) and before said step d),

- d1) encrypting said first authentication response in said at least one PSD (1040) after said step d) and before said step e), and

- e1) decrypting said first authentication response in said at least first Remote Computer System (1050) after said step e) and before said step f).

3. The method according to claim 1 or 2 for authenticating said at least one PSD (1040) vis-à-vis at least one subsequent Remote Computer System (1150) which is functionally connected to said at least first Remote Computer System (1050) through a second network, said method comprising the further steps of :

- aa) generating or retrieving, in said at least one subsequent Remote Computer System (1150), a second authentication challenge (1085),
- ab) transmitting said second authentication challenge (1085) from said at least one subsequent Remote Computer System (1150) to said at least first Remote Computer System (1050) via said second network,
- ac) converting said second authentication challenge (1085) in a PSD-formatted message,
- ad) transmitting said second authentication challenge (1085) from said at least first Remote Computer System (1050) to said at least one PSD (1040) through said at least one communications pipe (1075),
- ae) challenging said at least one PSD (1040) with said second authentication challenge, thereby generating a second authentication response,
- af) transmitting said second authentication response from said at least one PSD (1040) to said at least first Remote Computer System (1050) through said at least one communications pipe (1075),
- ag) transmitting said second authentication response from said at least first Remote Computer System (1050) to said at least one subsequent Remote Computer System (1150) via said second network, and
- ah) authenticating, in said at least one subsequent Remote Computer System (1150), said second authentication response.

4. The method according to claim 3, further comprising the steps of:

- ac1) encrypting said second authentication challenge (1085) in said at least first Remote Computer System (1050) after said step ac) and before said step ad),
- ad1) decrypting said second authentication challenge in said at least one PSD (1045) after said step ad) and before said step ae),
- ae1) encrypting said second authentication response in said at least one PSD (1040) after said step ae) and before said step af), and
- af1) decrypting said second authentication response in said at least first Remote Computer System (1050) after said step af) and before said step ag).

5. The method according to claim 1 or 2 for authenticating said at least one PSD (1040) vis-à-vis at least one subsequent Remote Computer System (1150) which is functionally connected to said at least first Remote Computer System (1050) through a second network, said method comprising the further steps of :

- ba) sending to said at least one PSD (1040) a credentials transfer command,
- bb) transmitting credentials (C) from said at least one PSD (1040) to said at least first Remote Computer System (1050) through said at least one communications pipe (1075),
- bc) storing said credentials (C, C') in said at least first Remote Computer System (1050),
- bd) generating or retrieving, in said at least one subsequent Remote Computer System (1050), a second authentication challenge (1085),
- be) transmitting said second authentication challenge (1085) from said at least one subsequent Remote Computer System (1050) to said at least first Remote Computer System (1010) via said second network,
- bf) challenging said stored credentials (C') with said second authentication challenge (1085), thereby generating a second authentication response,
- bg) transmitting said second authentication response from said at least first Remote Computer System (1050) to said at least one subsequent Remote Computer System (1150) via said second network, and
- bh) authenticating, in said at least one subsequent Remote Computer System (1150), said second authentication response.

6. The method according to claim 5, further comprising the steps of:

- ba1) encrypting said credentials (C) in said at least one PSD (1040) after said step ba) and before said step bb), and
- bb1) decrypting said credentials in said at least first Remote Computer System (1050) after said step bb) and before said step bc).

7. The method according to claim 1 or 2, comprising the step of initiating said communications pipe (1075) upon a request generated by said at least one Client (1010).

8. The method according to claim 1 or 2, comprising the step of initiating said communications pipe (1075) by at least one networked Remote Computer System.

9. The method according to claim 1, wherein PSD-formatted messages are APDU-formatted messages.

10. A Client (1010) for authenticating at least one PSD (1040) vis-à-vis at least a first Remote Computer System (1050) through at least one communications pipe (1075) established over a first network (1045) using said Client (1010) as a host to said at least one PSD (1040), wherein said Client (1010) comprises means (1015, 1025, 1105C) for transferring incoming and outgoing PSD-formatted messages (1260, 1270, 1460, 1470, 1360, 1370, 1560, 1570; 1660, 1670) between said at least one PSD (1040) and said at least first Remote Computer System (1050) through said at least one communications pipe (1075).

11. A Remote Computer System (1050) for authenticating at least one PSD (1040) vis-à-vis said Remote Computer System (1050) through at least one communications pipe (1075) established over a first network (1045) using said Client (1010) as a host to said at least one PSD (1040), wherein said Remote Computer System (1050) comprises means (1065) for:

- generating a first authentication challenge (1205), for transmitting said first authentication challenge (1205) to said at least one PSD (1040) through said communications pipe (1075) as an outgoing PSD-formatted message (1220, 1420), and for

- authenticating a first authentication response (1305) to said first authentication challenge (1205), said first authentication response (1305) being generated by said at least one PSD (1040) and transmitted to said Remote Computer System (1050) through said at least one communications pipe (1075) as an incoming PSD-formatted message (1320, 1520; 1620).

12. The Remote Computer System (1050) according to claim 11, further comprising cryptographic means (1225, 1325, 1425, 1525, 1625; 1725, 1825) for encrypting said outgoing PSD-formatted message (1220, 1420) and for decrypting said incoming PSD-formatted message (1320, 1520; 1620).

13. The Remote Computer System (1050) according to claim 11, further comprising means for:

- processing and routing to said at least one PSD (1040) through said at least one communications pipe (1075), as an outgoing PSD-formatted message, at least a second authentication challenge (1085) received over a second network from at least one subsequent Remote Computer System (1150), and for

- processing and routing to said at least one subsequent Remote Computer System (1150) at least a second authentication response to said at least second authentication challenge (1085), said at least second authentication response being generated by said at least one PSD (1040) and transmitted to said at least one subsequent Remote Computer System (1050) through said at least one communications pipe (1075) as an incoming PSD-formatted message (1520).

14. The remote Computer System (1050) according to claim 11, further comprising means for storing credentials (C') imported from said at least one PSD (1040) through said at least one communications pipe (1075) as an incoming PSD-formatted message (1620), and means for challenging said stored credentials (C') with at least a second authentication challenge (1085) received over a second network from at least one subsequent Remote Computer System (1150).

15. An authentication system, comprising at least one Client (1010) according to claim 10 and at least a first Remote Computer System (1050) according to claim 11 or 12 functionally connected to said at least one Client (1010) through said at least one communications pipe (1075).

16. An authentication system, comprising at least one Client (1010) according to claim 10 and at least a first Remote Computer System (1050) according to claim 13 or 14 functionally connected to said at least one Client (1010) through said at least one communications pipe (1075).

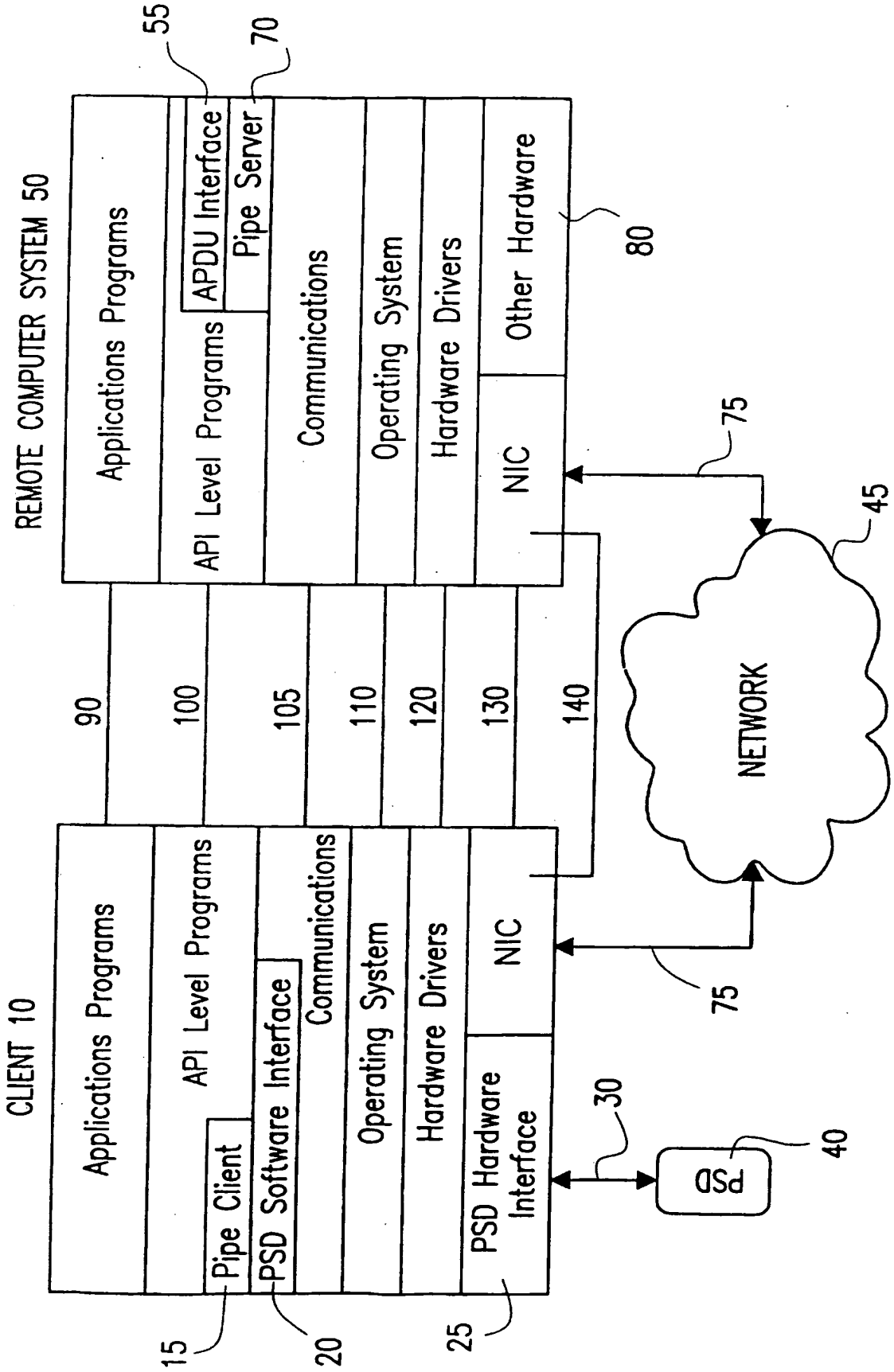
17. The authentication system according to claim 16, further comprising said at least one subsequent Remote Computer System (1150) functionally connected to said at least first Remote Computer System (1050) through said second network, wherein said at least one subsequent Remote Computer System (1150) comprises means (1095) for generating said at least second authentication challenge (1085), for transmitting said at least second authentication challenge (1085) to said at least first Remote Computer System (1050) through said second network and for

authenticating said at least second authentication response to said at least second authentication challenge (1085).

18. The authentication system according to claim 17, further comprising said at least one PSD (1040), wherein said at least one PSD (1040) comprises authentication means for generating said first response (1035) to said first authentication challenge (1205).

19. The authentication system according to claim 16, wherein said first (1045) and second networks form one same network.

FIG.1



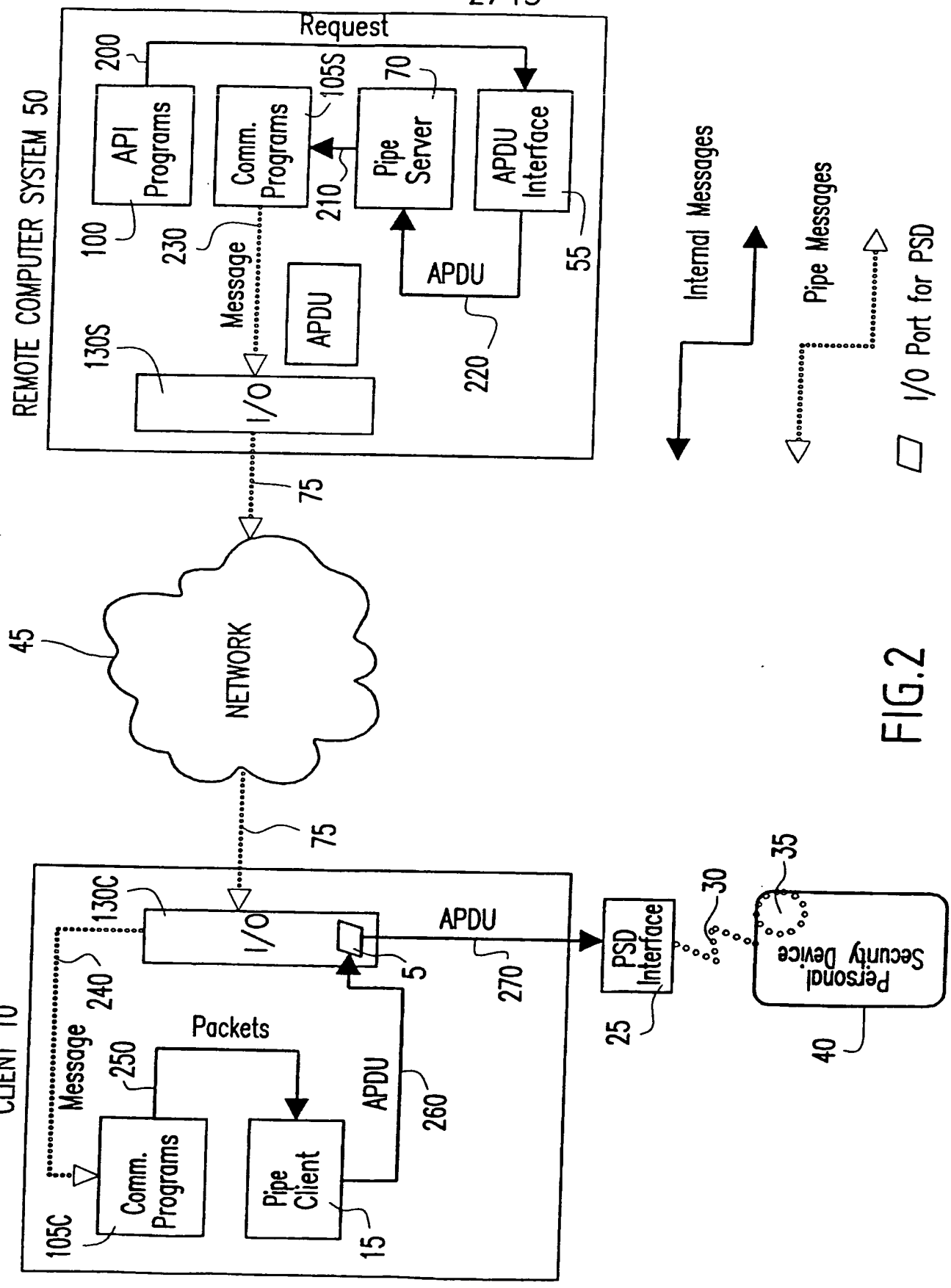


FIG.2

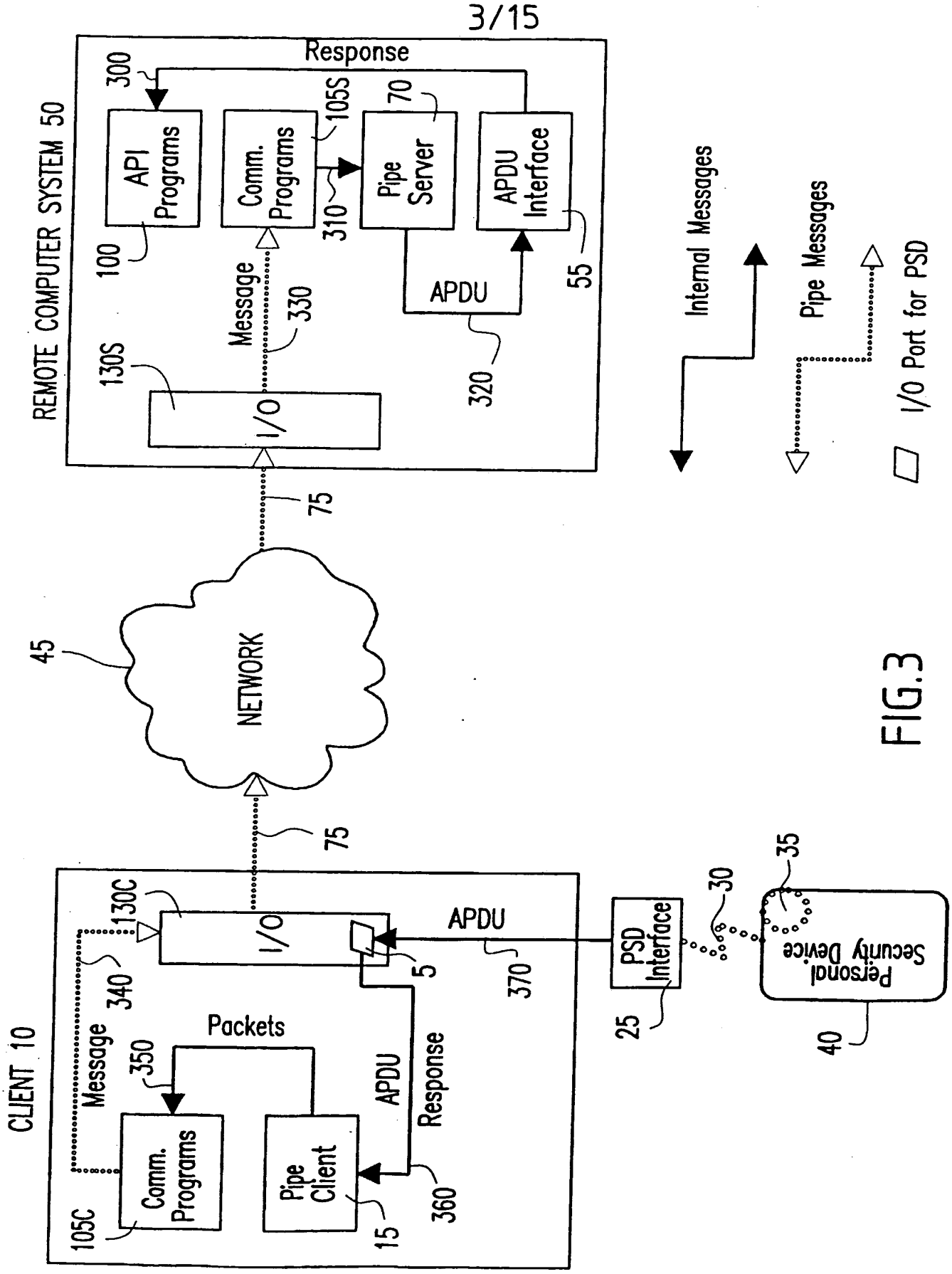

REMOTE COMPUTER SYSTEM 50
Response
300
API Programs
100
Comm. Programs
105S
310
Pipe Server
70
APDU Interface
55
Message
330
APDU
320
130S
I/O
75
NETWORK
45
75
CLIENT 10
130C
I/O
APDU
370
5
340
Message
Packets
350
Comm. Programs
105C
Pipe Client
15
APDU
Response
360
PSD Interface
25
30
35
Personal Security Device
40
Internal Messages
Pipe Messages
I/O Port for PSD

FIG.3

FIG.4A

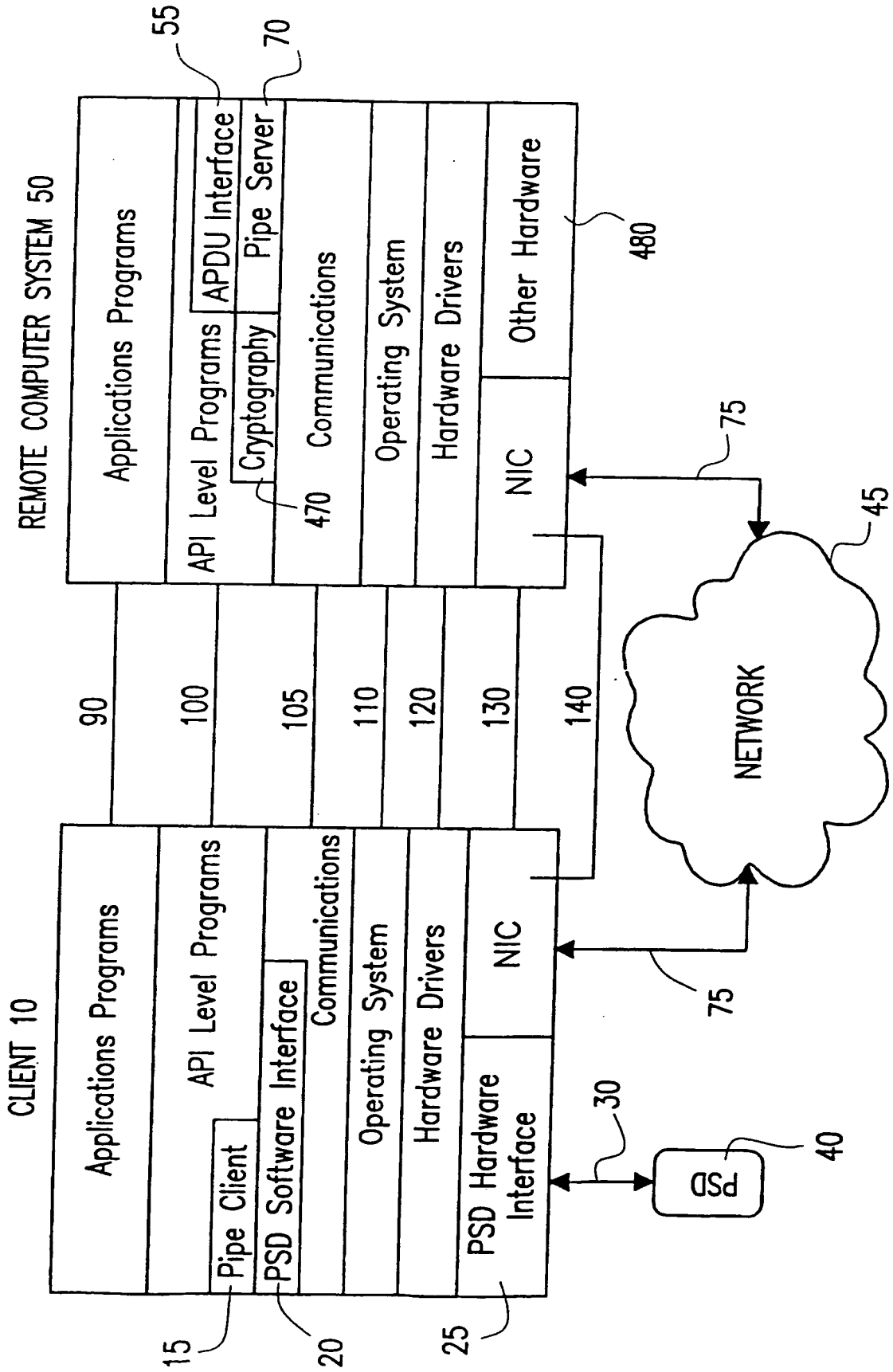
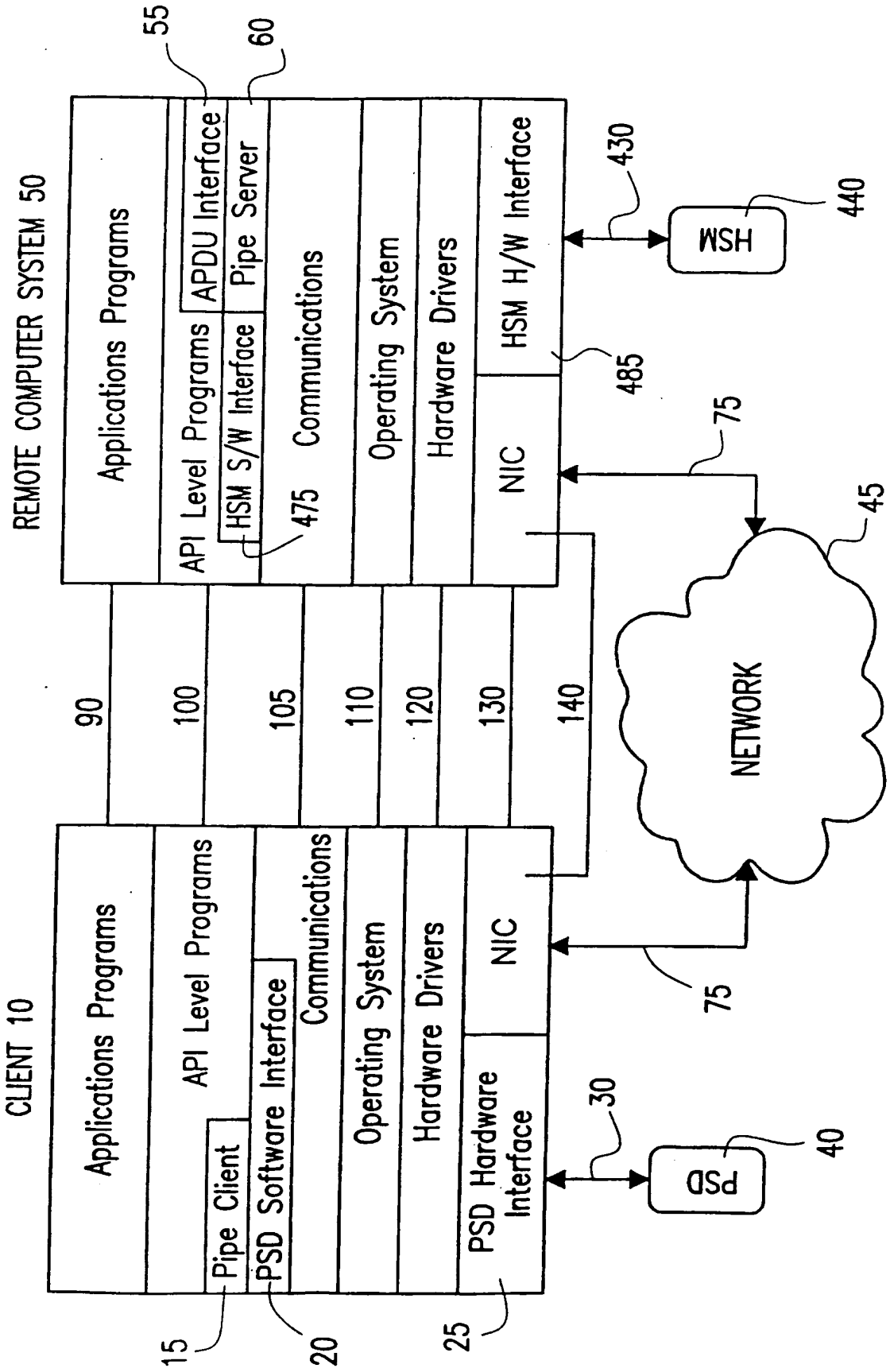


FIG.4B



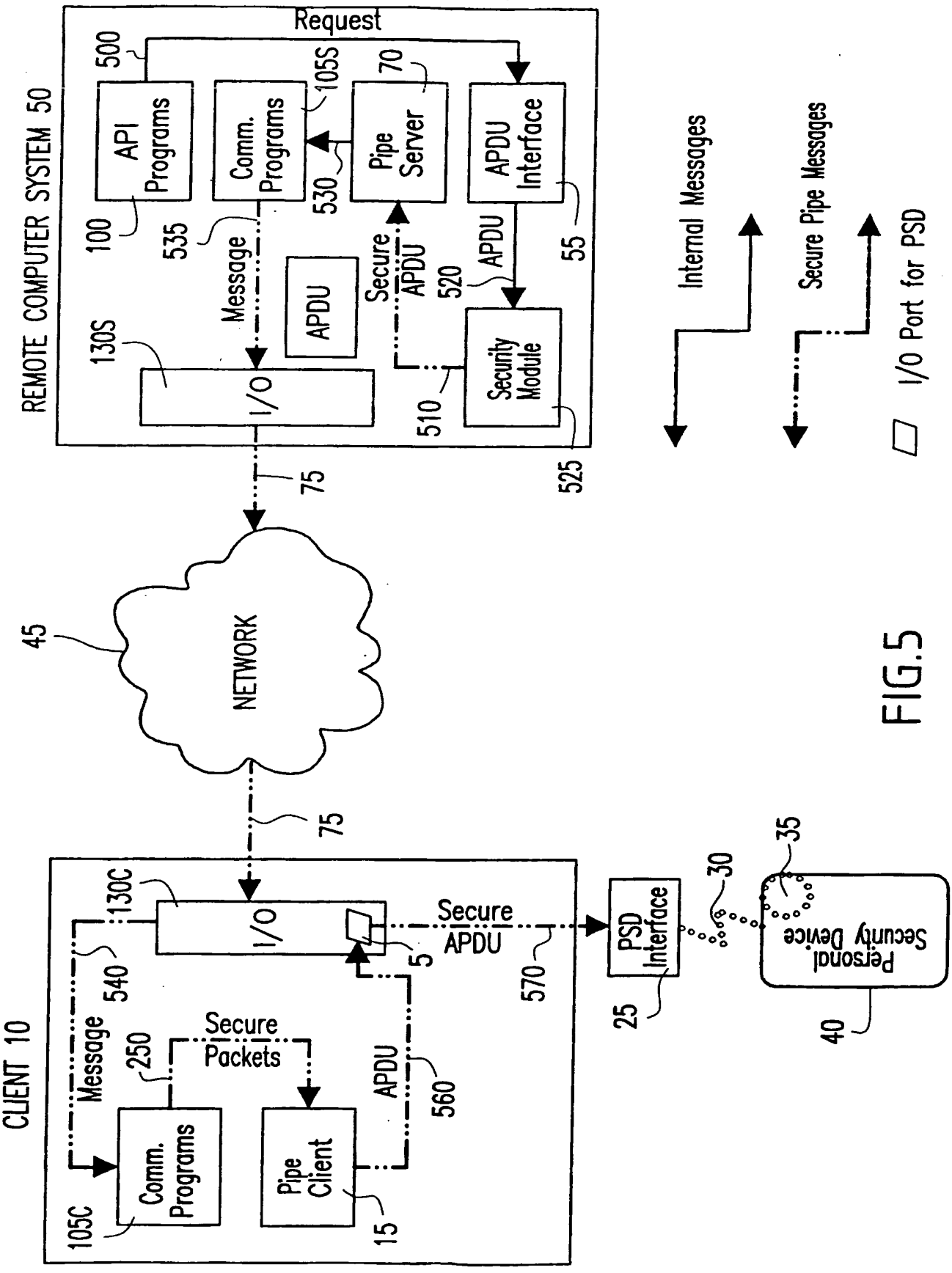

REMOTE COMPUTER SYSTEM 50
Request
500
API Programs
100
Comm. Programs
105S
535
Message
Pipe Server
70
530
APDU Interface
55
APDU
Secure APDU
520
APDU
130S
I/O
510
Security Module
525
75
45
NETWORK
75
CLIENT 10
130C
I/O
Secure APDU
5
570
540
Message
250
Secure Packets
APDU
560
Comm. Programs
105C
Pipe Client
15
PSD Interface
25
30
35
Personal Security Device
40
Internal Messages
Secure Pipe Messages
I/O Port for PSD

FIG.5

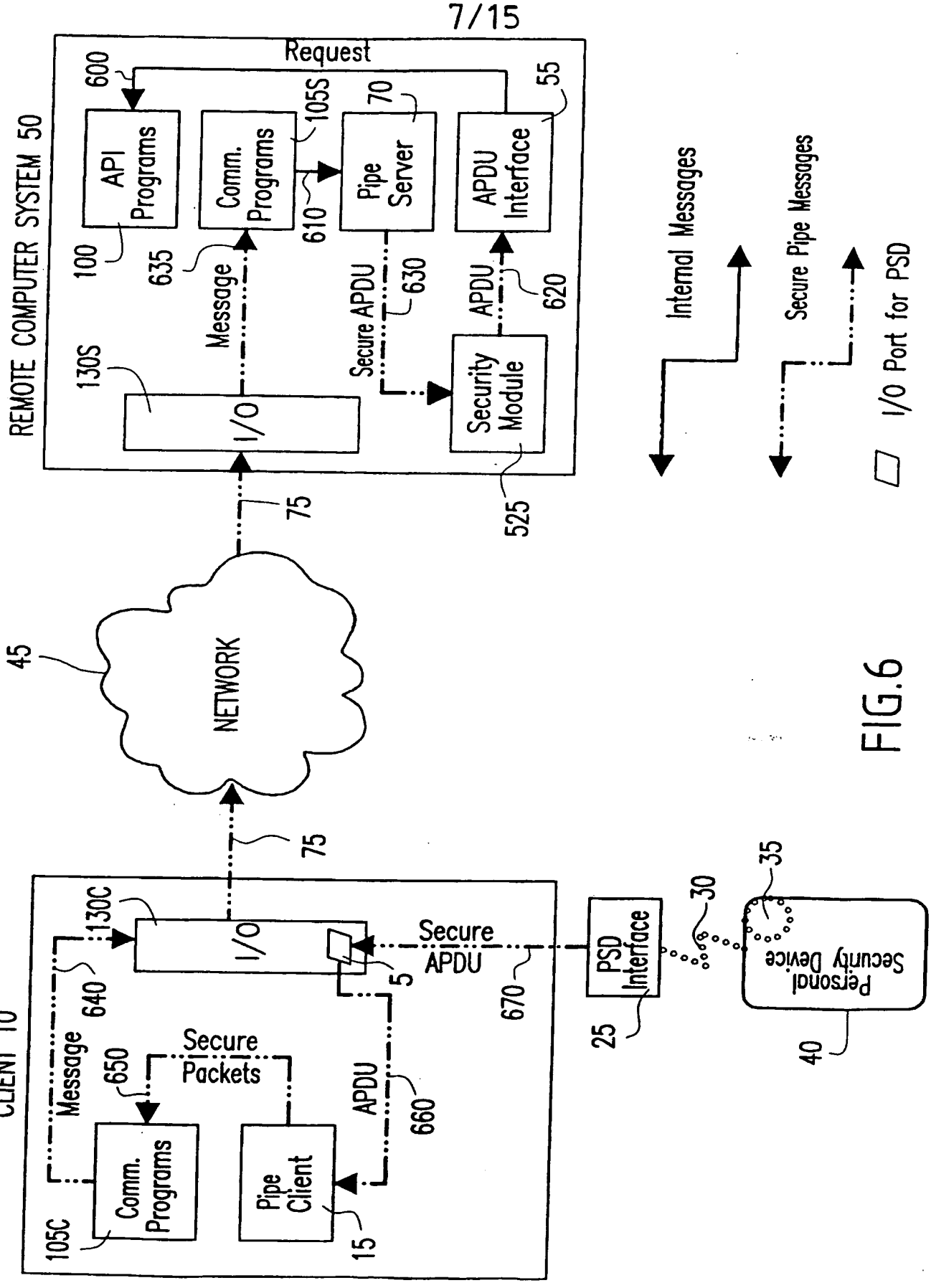
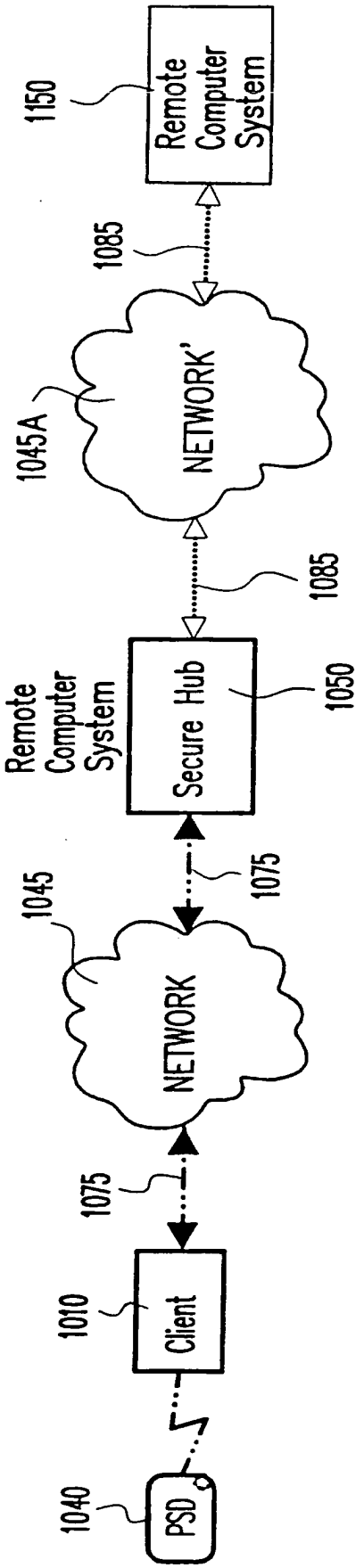

REMOTE COMPUTER SYSTEM 50
Request
600
API Programs
100
Comm. Programs
105S
635
Message
Pipe Server
610
Secure APDU
630
APDU Interface
55
APDU
620
130S
I/O
Security Module
525
75
NETWORK
45
75
CLIENT 10
130C
I/O
640
Message
Secure APDU
5
670
650
Secure Packets
APDU
660
105C
Comm. Programs
Pipe Client
15
PSD Interface
25
30
35
Personal Security Device
40
Internal Messages
Secure Pipe Messages
I/O Port for PSD

FIG.6



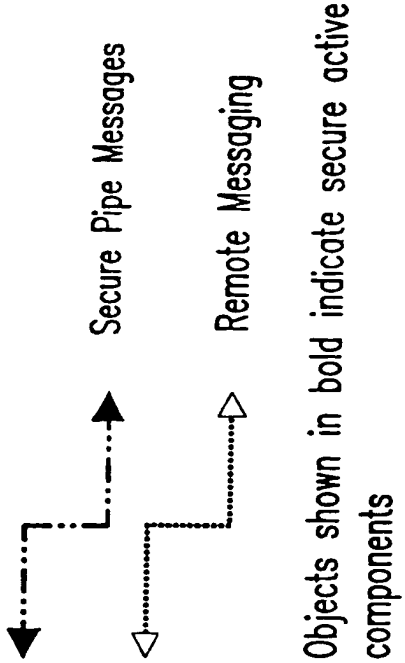


FIG.7

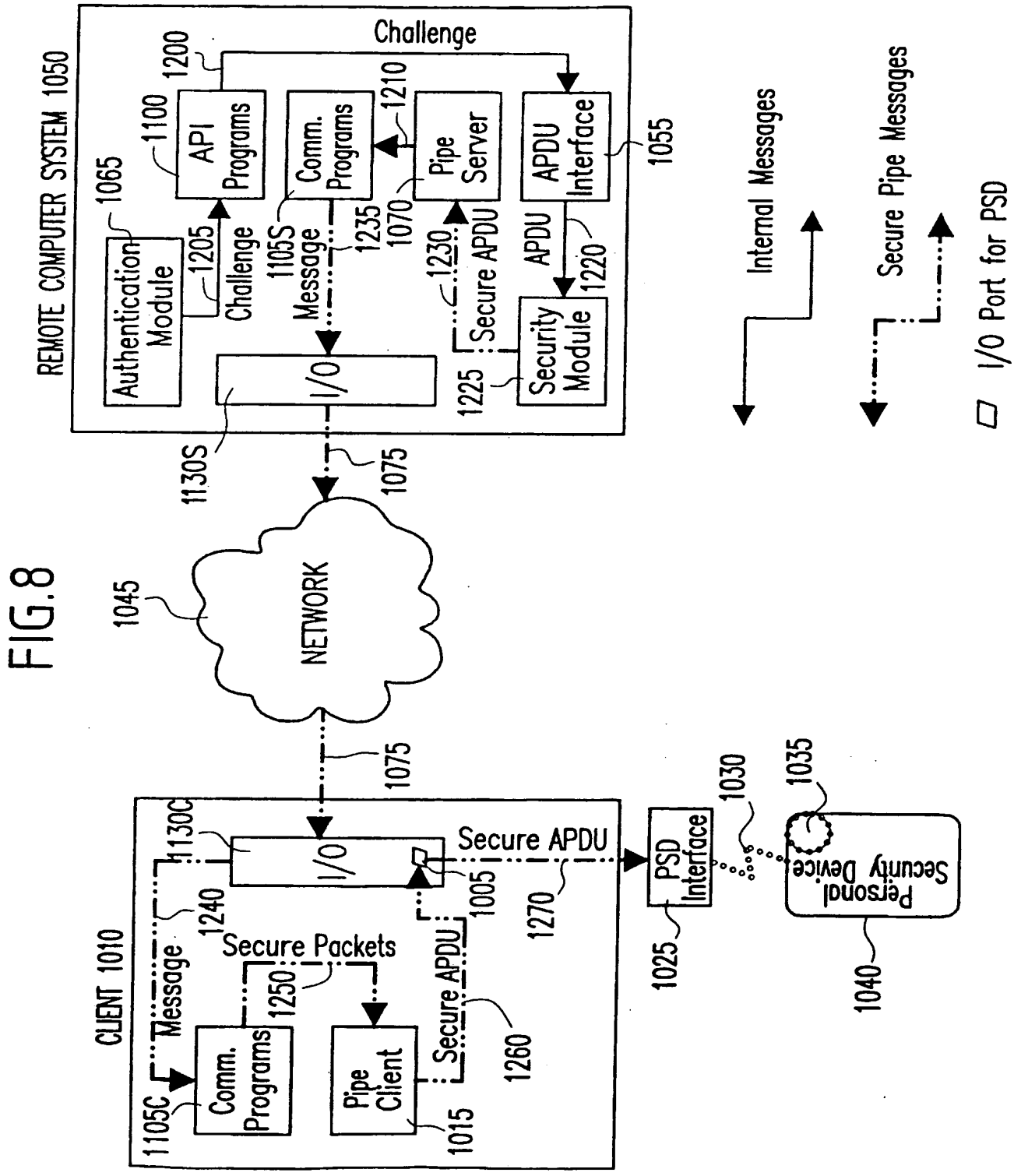

REMOTE COMPUTER SYSTEM 1050
Challenge
1200
API Programs
1100
Comm. Programs
1210
Pipe Server
APDU Interface
1055
Authentication Module
1065
1205
Challenge
1105S
Message
1235
1070
1230
Secure APDU
APDU
1220
Security Module
1225
I/O
1130S
1075
NETWORK
1045
Internal Messages
Secure Pipe Messages
I/O Port for PSD
CLIENT 1010
1130C
I/O
Secure APDU
1005
1270
PSD Interface
1030
1035
Personal Security Device
1240
Message
Secure Packets
1250
Secure APDU
1260
1105C
Comm. Programs
Pipe Client
1015
1025
1040

FIG.8

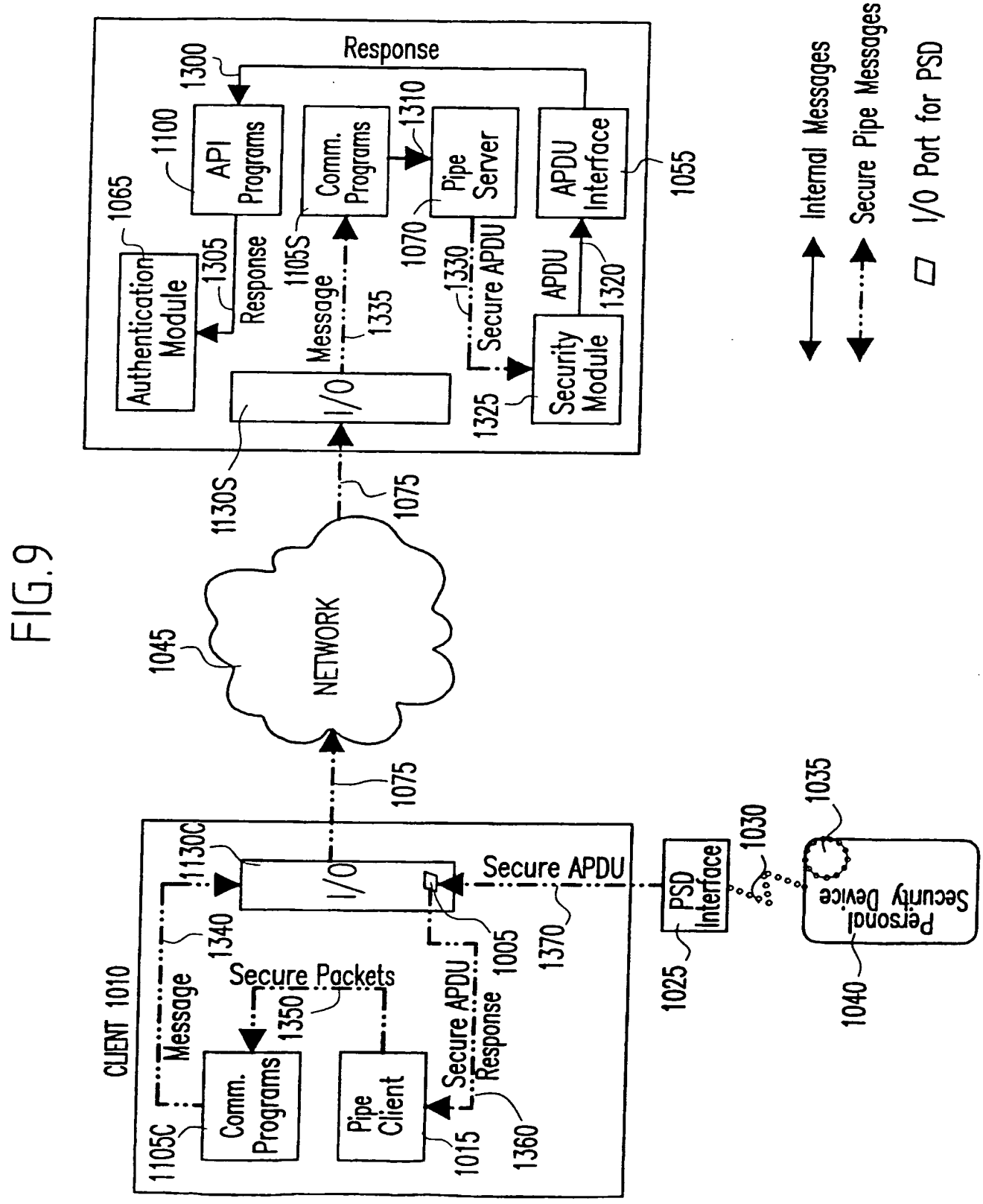


FIG.9

FIG.10

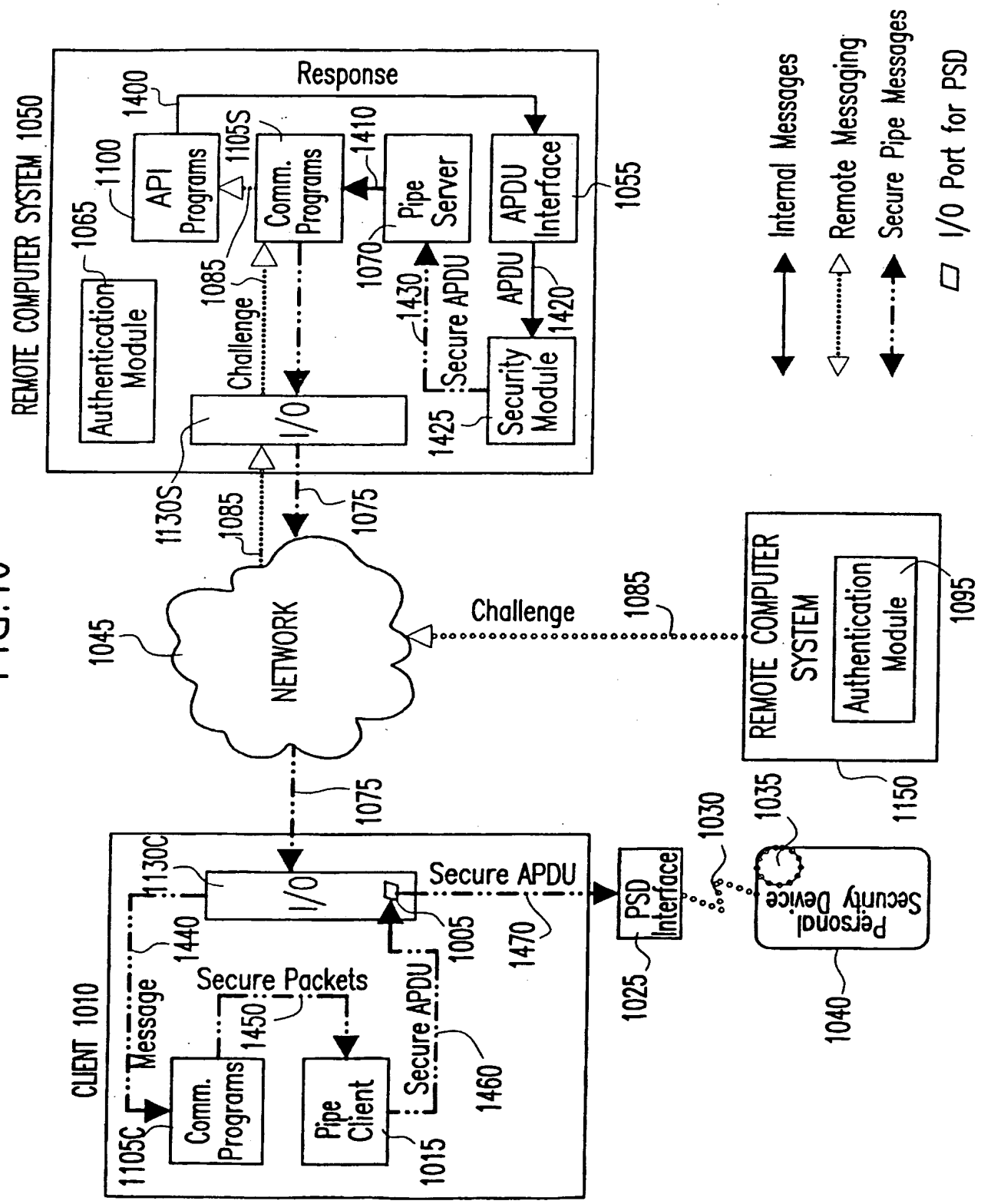

REMOTE COMPUTER SYSTEM 1050
Response
1400
API Programs
1100
1105S
Comm. Programs
1410
Pipe Server
APDU Interface
1055
1065
Authentication Module
1085
Challenge
1070
1430
Secure APDU
APDU
1420
Security Module
1425
I/O
1130S
1085
1075
NETWORK
1045
Challenge
1085
REMOTE COMPUTER SYSTEM
Authentication Module
1095
1150
1075
1130C
I/O
Secure APDU
1440
1005
1470
PSD Interface
1030
1035
Personal Security Device
1025
1040
CLIENT 1010
Message
Secure Packets
1450
Secure APDU
1460
1105C
Comm. Programs
Pipe Client
1015
Internal Messages
Remote Messaging
Secure Pipe Messages
I/O Port for PSD

FIG.11

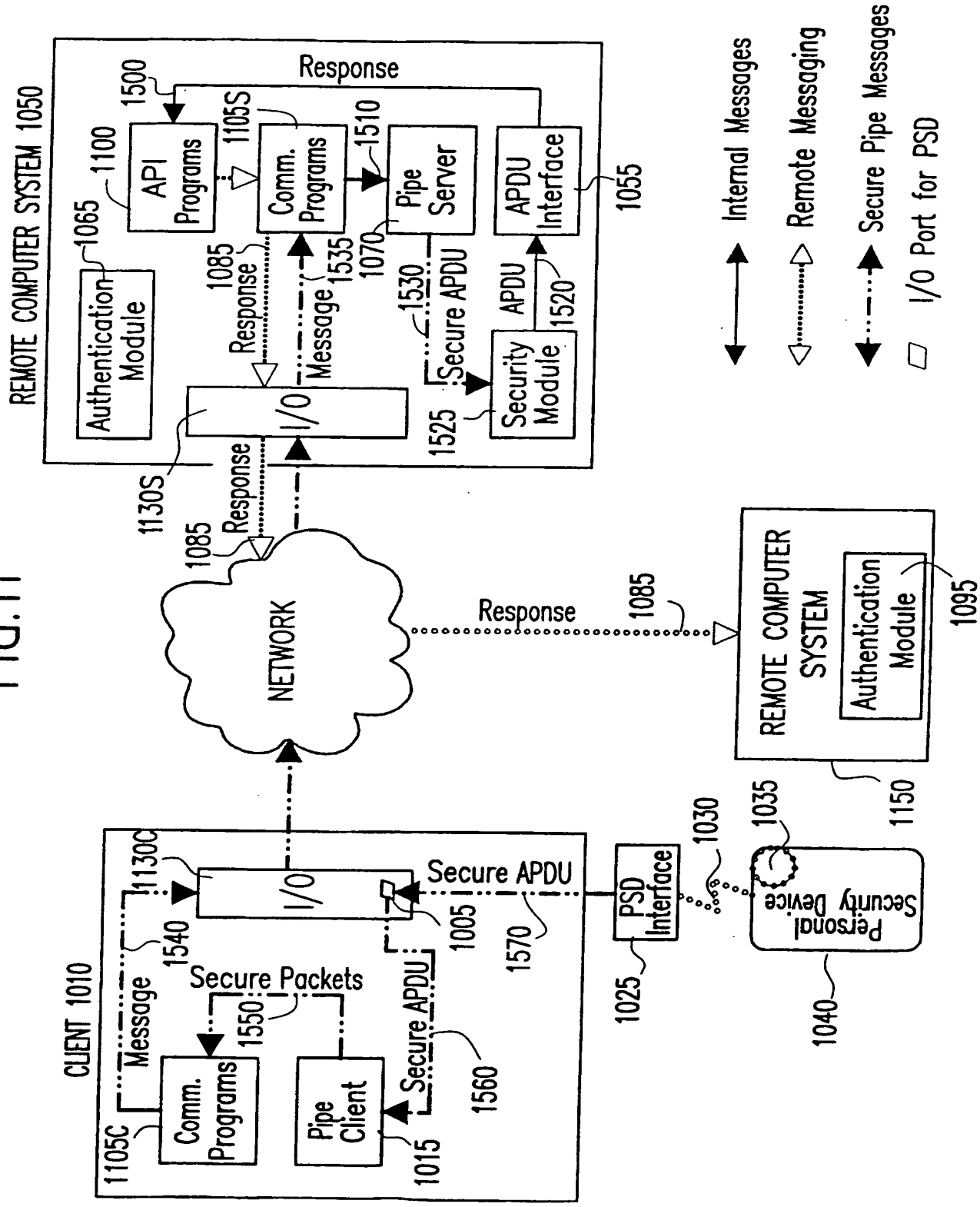


FIG.12

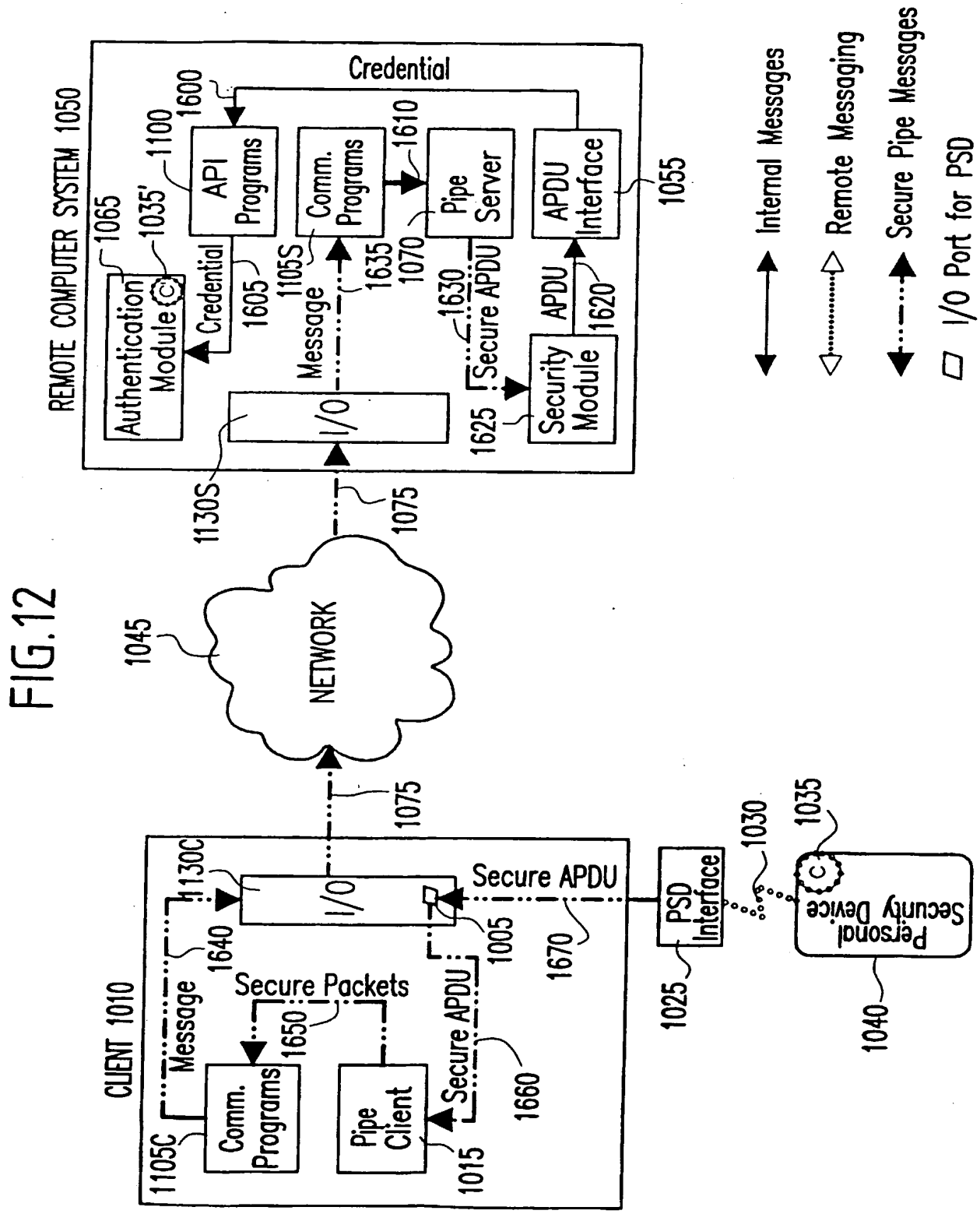


FIG.13

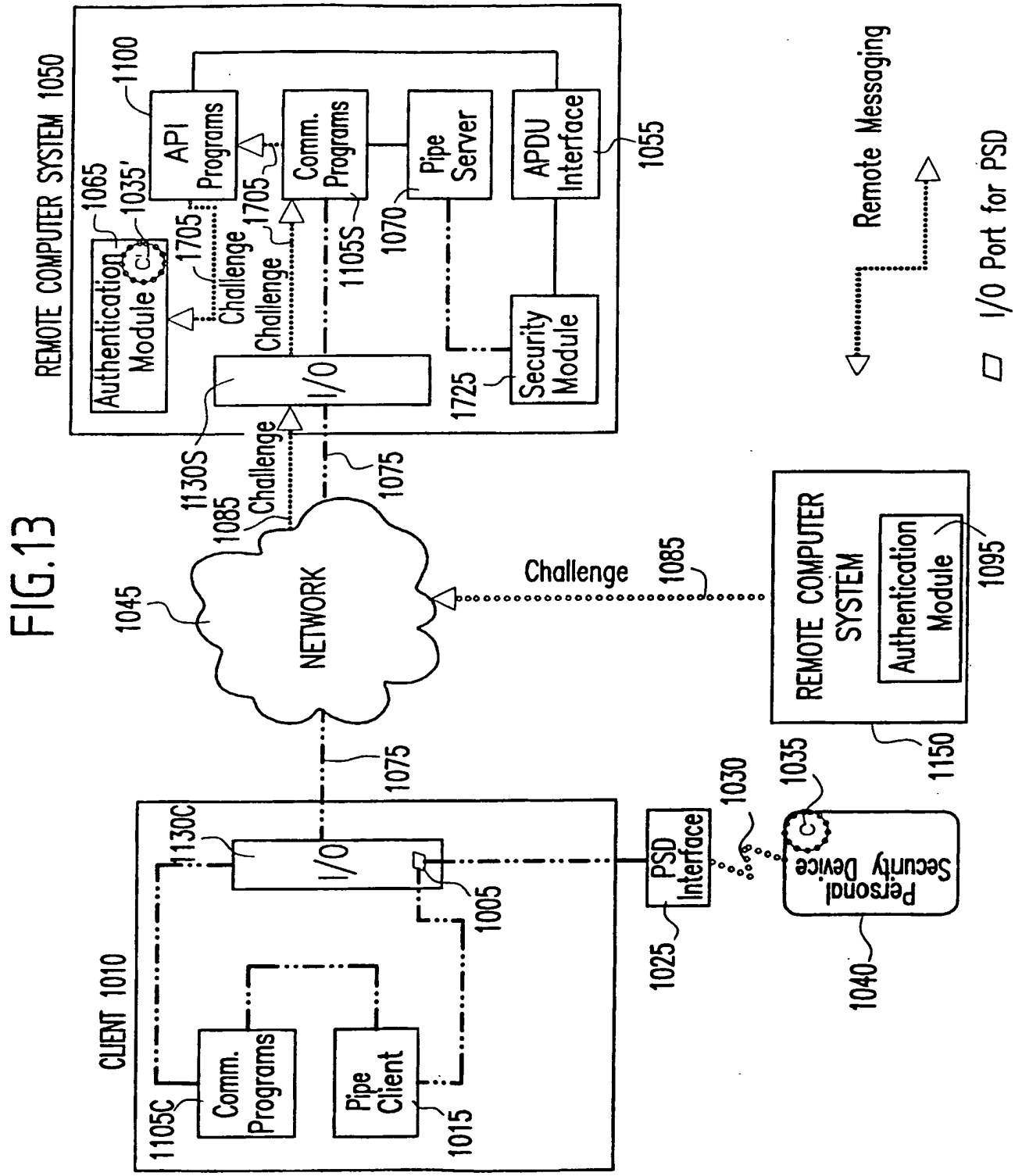
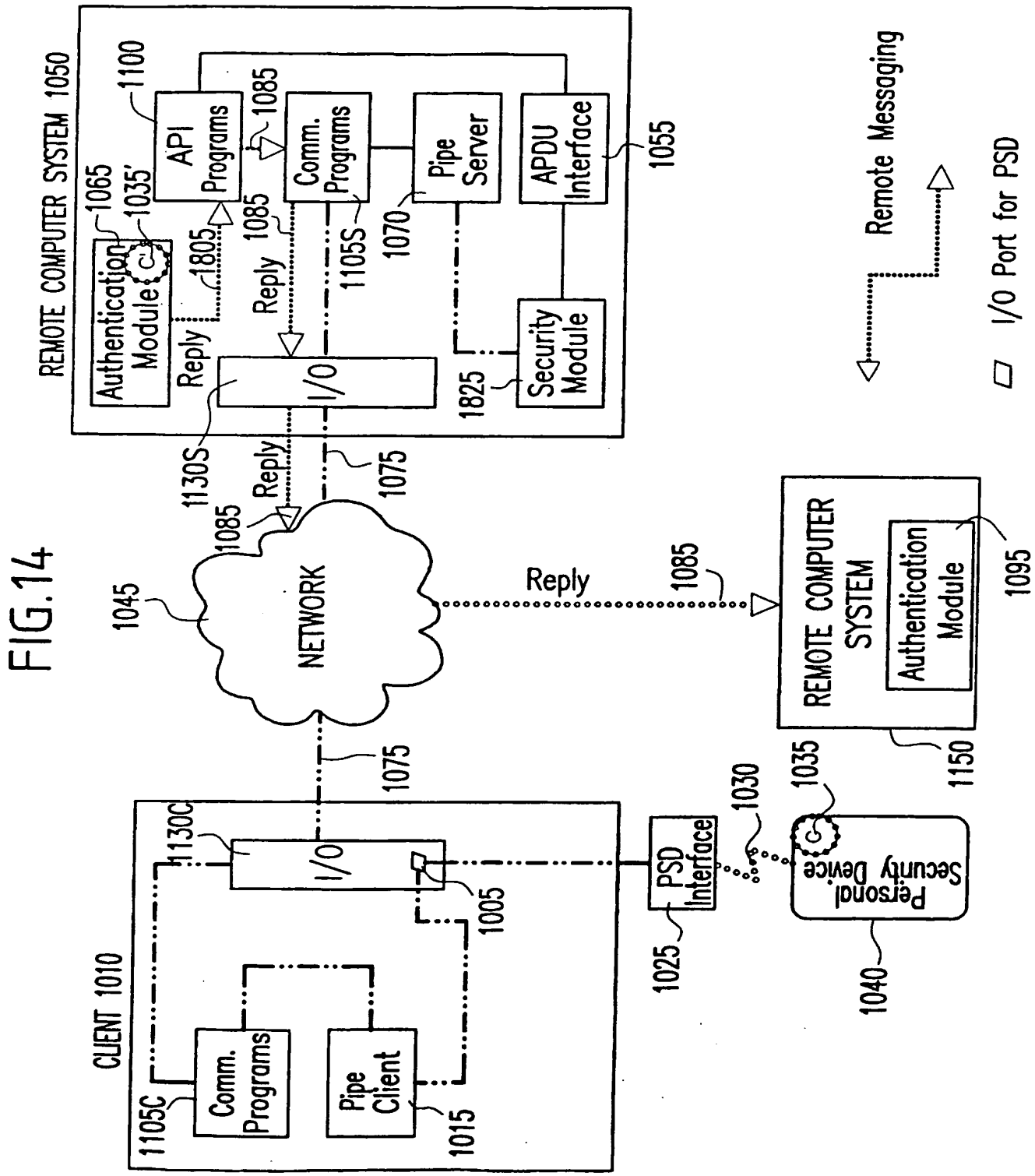


FIG.14



INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 02/03929

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04L9/32 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, COMPENDEX, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 778 071 A (AMORUSO VICTOR P ET AL) 7 July 1998 (1998-07-07) figures 2,3,5A column 1, line 10-14 column 2, line 23 - line 47 column 5, line 8 - line 44 column 12, line 23 - line 29 column 13, line 25 -column 14, line 9 column 15, line 13 - line 33 ---	1-4, 7-13,15, 16
P,X A	US 2002/025046 A1 (HUNG-YU LIN) 28 February 2002 (2002-02-28) figures 9-18 paragraphs '0021!-'0023! paragraphs '0036!-'0046! --- -/--	1-4, 7-13,15, 16 5,6,14, 17-19

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 August 2002	27/08/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Bub, A

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 02/03929

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 01 22373 A (HEIDEN PAUL RICHARD ;KROP HILDEBRAND RUBEN (NL); WACHEM PAUL ANTHO) 29 March 2001 (2001-03-29) page 10, line 10 - line 25 page 12, line 1 - line 2 ---	5,6,14, 17-19
A	WO 01 16900 A (AMERICAN EXPRESS TRAVEL RELATE) 8 March 2001 (2001-03-08) page 8, line 5 - line 27 page 26, line 13 - line 20 figures 10,11 ---	5,6,14, 17-19
A	EBRINGER T ET AL: "PARASITIC AUTHENTICATION TO PROTECT YOUR E-WALLET" COMPUTER, IEEE COMPUTER SOCIETY, LONG BEACH., CA, US, US, vol. 33, no. 10, 1 October 2000 (2000-10-01), pages 54-60, XP001001747 ISSN: 0018-9162 the whole document -----	5,6,14, 17-19

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 02/03929

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5778071 A	07-07-1998	US 5546463 A	13-08-1996
		AU 726397 B2	09-11-2000
		AU 4147097 A	06-03-1998
		EP 0916210 A1	19-05-1999
		WO 9807255 A1	19-02-1998
		US 5878142 A	02-03-1999
US 2002025046 A1	28-02-2002	NONE	
WO 0122373 A	29-03-2001	AU 3844900 A	24-04-2001
		EP 1221145 A1	10-07-2002
		WO 0122373 A1	29-03-2001
WO 0116900 A	08-03-2001	AU 7090700 A	26-03-2001
		BR 0013822 A	23-07-2002
		EP 1212732 A2	12-06-2002
		NO 20020996 A	24-04-2002
		WO 0116900 A2	08-03-2001